

What is claimed is:

- 1 1. A processor comprising:
2 a mechanism to identify memory as secure memory accessible by secure
3 processes, and to identify non-secure memory accessible by both secure and non-
4 secure processes; and
5 a security enforcement mechanism to allow page tables for the non-secure
6 processes to be stored in secure memory.
- 1 2. The processor of claim 1 wherein the processor can operate in a secure mode
2 and in a non-secure mode; and the security enforcement mechanism allows page
3 table walks for non-secure processes while in non-secure mode.
- 1 3. The processor of claim 1 wherein the security enforcement mechanism
2 includes page table walk hardware capable of walking page tables in secure memory
3 in response to architecture events caused by non-secure processes.
- 1 4. The processor of claim 1 wherein the security enforcement mechanism
2 includes circuits to differentiate between program generated memory accesses and
3 architecture generated memory accesses, and to block program generated memory
4 access from accessing secure memory.
- 1 5. The processor of claim 1 further comprising a configurable memory
2 management unit capable of requiring non-secure process to access secure memory
3 when performing page table walks.
- 1 6. The processor of claim 1 further comprising virtual address translation
2 hardware to perform virtual address translation for non-secure processes via page
3 tables in secure memory.

1 7. The processor of claim 1 further comprising a translation look-aside buffer
2 (TLB), wherein the security enforcement mechanism allows a secure memory
3 access after a TLB miss.

1 8. The processor of claim 1 further comprising a control register to specify
2 whether page tables for non-secure processes are kept in secure memory or non-
3 secure memory.

1 9. The processor of claim 1 further comprising page table walk hardware
2 capable of accessing secure memory on behalf of non-secure processes.

1 10. A processor comprising an apparatus to differentiate between hardware
2 generated memory accesses and software generated memory accesses and to grant
3 secure memory access to hardware generated memory accesses.

1 11. The processor of claim 10 wherein the hardware generated memory accesses
2 are the result of a translation look-aside buffer (TLB) miss.

1 12. The processor of claim 11 wherein hardware generated memory accesses
2 may be caused by secure or non-secure processes.

1 13. The processor of claim 10 wherein the hardware generated memory accesses
2 are the result of architecture events.

1 14. The processor of claim 13 wherein the architecture events result in a page
2 table walk for a non-secure process.

1 15. A processor comprising circuitry to differentiate between non-secure process
2 having page tables in non-secure memory, secure processes capable of having page

3 tables in non-secure memory or secure memory, and safer secure processes having
4 page tables in secure memory.

1 16. The processor of claim 15 wherein the circuitry comprises a memory
2 management unit.

1 17. The processor of claim 16 wherein the memory management unit comprises
2 a control register to prevent the processor from using non-secure memory when
3 performing a page table walk for a secure process.

1 18. The processor of claim 15 further comprising page table walk hardware to
2 perform page table walks.

1 19. The processor of claim 18 wherein the processor can operate in a secure
2 mode or non-secure mode, and the page table walk hardware can perform page table
3 walks without changing the mode in which the processor operates.

1 20. A method comprising:
2 determining if a translation look-aside buffer (TLB) miss has occurred;
3 determining if a current process page table is in secure or non-secure
4 memory; and
5 if the current process page table is in secure memory, performing a page
6 table walk in secure memory.

1 21. The method of claim 20 wherein the page table walk is performed for a
2 secure process.

1 22. The method of claim 20 wherein the page table walk is performed for a non-
2 secure process.

1 23. The method of claim 20 further comprising if the current process page table
2 is in non-secure memory, performing the page table walk in non-secure memory.

1 24. An electronic system comprising:
2 a plurality of antennas;
3 an amplifier coupled to at least one of the plurality of antennas to amplify
4 communications signals;
5 a processor coupled to the amplifier; and
6 memory that can be partitioned by the processor into secure memory
7 accessible by secure processes and non-secure memory accessible by secure or non-
8 secure processes;
9 wherein the processor includes a security enforcement mechanism to allow
10 page tables for non-secure processes to be stored in secure memory.

1 25. The electronic system of claim 24 wherein:
2 the processor can operate in a secure mode and in a non-secure mode; and
3 the security enforcement mechanism allows page table walks for non-secure
4 processes while in non-secure mode.

1 26. The electronic system of claim 24 wherein the security enforcement
2 mechanism includes page table walk hardware capable of walking page tables in
3 secure memory in response architecture events caused by non-secure processes.